UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,980	11/14/2003	Brian D. Swander	14917.0474US01	3167

27488 7590 08/10/2007

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,980	SWANDER ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 18-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 18-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 10/2/06, 10/3/06, 10/19/06 11/1/06, 11/14/03
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 18-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim recites "computer-readable medium for executing computer-readable instructions....". The Office interprets the intended use clause reciting in the claims would preempt the claims to software or program modules, and therefore reciting non-statutory subject matter. The subject matter is statutory if the computer instructions/programs are residing on a computer readable medium and are executed in a processor and produce a useful, concrete and tangible result.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-9 and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faucher (5,515,441) in view of Inoue et al (6,170,057 B1).

In reference to claims 1 and 18, Faucher discloses a communication system in which a node may communicate over insecure channels with any of a plurality of terminals (abstract). Faucher teaches conducting a main mode, certificate exchange, negotiation for establishing the secure path (column 10 lines 1-13); conducting a quick mode, Diffie Helman key exchange, negotiation for deriving a set of keys usable with the security protocol (column 10 line 13 to column 11 line 2). Wherein at least a portion of the quick mode occurs during the main mode and a quick mode pseudo random number is exchanged between the responder and the initiator (column 10 line 13 to column 11 line 2).

However Faucher does not expressly disclose selecting the set of security parameters including a security protocol and establishing inbound and outbound protocol security association.

Inoue teaches a mobile computer and a packet encryption and authentication method which are capable of controlling an activation of a packet encryption and authentication device belonging to the mobile computer according to the security policy at the visited network (abstract). Inoue teaches negotiation for establishing the secure path and selecting the set of security parameters including a security protocol (column 7 lines 1-11). And wherein a protocol security process establishes inbound and outbound protocol security associations (column 7 lines 20-29.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer

terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to claim 2 and 19 Faucher teaches further comprising conducting a first user mode for authenticating a first user associated with the initiator or responder (column 10 lines 1-10).

In reference to claims 3 and 20 Faucher teaches a system wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the main mode (column 10 lines 3-8).

In reference to claim 4 the system of Faucher comprising conducting a second user mode for authenticating a second user associated with the initiator or the responder (column 10 lines 1-10).

In reference to claim 5 Faucher does not discloses a system wherein a set of proposed security parameters are used for selection of the parameters used for communication.

The system of Inoue discloses a system wherein the main mode comprises sending the initiator to the responder, a set of proposed security parameters and authentication data; selecting, by the responder, the set of security parameters from the set of proposed security parameters; and sending the set of security parameters from the responder to the initiator (column 7 lines 20-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because

due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to claims 6 and 21 Faucher teaches a system wherein the initiator identifies a public key of the responder prior to the main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key (Fig 6).

In reference to claim 8 Faucher teaches further comprising exchanging Diffie Hellman key data between the initiator and the responder during main mode for deriving keys for use with an encryption algorithm (column 10 lines 1-20).

In reference to claim 9 Faucher does not disclose exchanging a pair of notify payloads between the initiator and the responder wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations.

further comprising exchanging a pair of notify payloads between the initiator and the responder; wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less

centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to claims 7 and 22 Faucher does not disclose the mode wherein a group advertisement from the initiator to the responder; and comparing the group advertisement to a set of authorized groups; and sending a response from the responder to the initiator. The group advertisement corresponds to the security parameters of the remote network gateway.

Inoue discloses a system wherein the main mode comprises sending a group advertisement from the initiator to the responder; and comparing the group advertisement to a set of authorized groups; and sending a response from the responder to the initiator (column 7 lines 20-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK
August 6, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100